REMARKS

Claims 34-53 are pending in this application. Claims 1-33 have been cancelled. Claims 34-53 have been added in this response. Claims 34, 48, and 51 are the independent claims in this case. It is believed that no new matter has been added by this amendment.

Claims 1, 3-4, 6-12, 16-29, and 31-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication Number 2002/0144156 to Copeland ("Copeland") in view of U.S. Patent Number 6,769,066 to Botros et al. ("Botros"). In view of the amendments and remarks presented herein, the undersigned respectfully traverses these rejections as set forth below. The undersigned will address each independent claim separately as the Applicant believes that each independent claim is separately patentable over the prior art of record.

While the Applicant has added new claims to this patent application which have not been considered by the Examiner, these claims are based on and include many of the elements of the previously rejected claims and therefore, the Applicant has addressed these claims with respect to the current prior art of record. The Applicant thanks Examiner Jackson for her suggestion of how the claims of this case should be amended as noted in her last Office Action of December 31, 2007. In that Office Action, Examiner Jackson suggested several elements to be claimed by the Applicant which included outputting a behavioral rating and the behavioral rating comprising at least two dimensions of deception and expertise. The Applicant notes that these elements are now positively recited in the current new claims.

Independent Claim 34

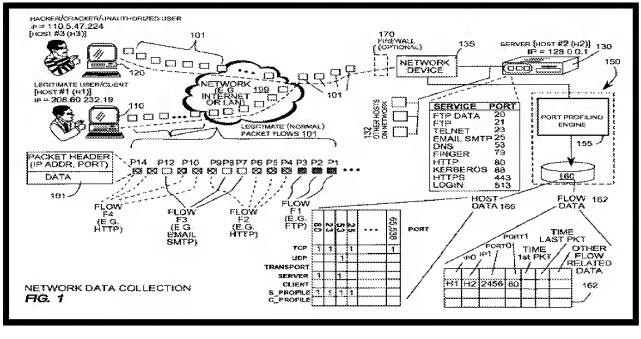
It is respectfully submitted that Copeland and Botros, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) copying packets that are being transmitted in real-time over the computer network; (2) sorting the copied packets based on port type; (3) sending packets of a particular type to one or more port modules, (4) each port module being designed for processing packets of a single port type; (5) processing packets with each port module by reviewing and comparing information from various parts of each packet; (6) determining a presence and absence of port-specific activities based on each packet with each port module; (7) generating binary vectors representing the presence and absence of port-specific

activities based on each packet with each port module; (8) assessing each binary vector and determining a level of expertise and deception for the port-specific activities represented by the binary vector with each port module; and (9) outputting a behavioral rating from each port module in real-time based on the assessing and determining steps, the behavioral rating comprising at least two dimensions of deception and expertise, as recited in independent Claim 34.

Support for these steps can be found in paragraphs [0034-0035] and [0038-0039] of the published, original application as filed.

Copeland

Copeland describes a port profiling engine 155 which monitors network computer communications. The network computer communications are routed via a known global computer network commonly known as the Internet 199. The port profiling engine 155 is incorporated into a monitoring appliance 150, together with a database 160 that stores information utilized in the port profiling methodology. Copeland, paragraph [0037]. The engine 155 collects port information associated with each flow and stores this information in a database 160. As illustrated in Figure 1 of Copeland (reproduced below), the database 160 comprises a flow data structure 162 and a host data structure 166. Copeland, paragraph [0054].



The flow data structure 162 of Copeland stores collected flow information such as the IP addresses. The engine 155 determines which host has a lower IP address and assigns that host IP0. The other host is assigned IP1. Port0 is associated with IP0 and port1 is the service connection port for IP1. The flow data structure 162 also stores time and other related packet information derived from the packet header. This time information (e.g. time of the first packet, time of the last packet) is utilized to measure the elapse of time for purposes of flow delimiting. Copeland, paragraph [0055].

The host data structure 166 of Copeland maintains the port profiling information. Port profiling entails keeping two lists for each of the hosts: 1) a list by port number (0, 65,536), protocol (TCP or UDP), and type of operation (client or server) for all allowed network services that are in the hosts profile; and 2) a corresponding list of network services that have been seen today. Copeland, paragraph [0056].

Copeland explains that the port profiling engine 155 does not analyze the data segments of packets for signature identification. Instead, the engine 155 associates all packets with a flow. It analyzes certain statistical data and tracks the associated network services. The engine 155 compares recent activity to a predetermined port profile. An alarm is generated when a host uses a service that is not in its port profile. Copeland, paragraph [0103].

The Examiner admits that Copeland fails to describe or teach behaviors and activities for each IP/user and processing in real-time the presence or absence of identified behavior elements. The Examiner also suggested in her last Office Action that the Applicant should amend the claims to recite the elements of a behavioral rating and the behavioral rating comprising at least two dimensions of deception and expertise, which are clearly not taught by Copeland. The Applicant has amended the claims to recite these elements.

The Applicant also points out that Copeland further fails to teach or describe copying packets that are being transmitted in real-time over the computer network, sending packets of a particular port type to one or more port modules, each port module being designed for processing packets of a single port type; and processing packets with each port module by reviewing and comparing information from various parts of each packet, as recited in independent Claim 34.

One of ordinary skill in the art recognizes that Copeland is designed to monitor packets at a higher level relative to Applicant's claimed invention. Copeland does not process packets with

port modules designed for a single port type and Copeland does not review and compare information from various parts of each packet, as recited in amended independent Claim 34. Paragraph [0103] of Copeland is evidence that Copeland is only concerned with certain statistical data and the tracking of associated network services, which is not the same as the claimed invention.

Botros

To address the several deficiencies of Copeland, the Examiner relies upon Botros. Botros describes a computer network security system 100 that tracks user activity files 12. These files contain raw user data generated from various system resources and are parsed and organized according to user and time of activity. Botros explains that historical data 102 contains data relating to prior activity performed by a user and cumulative data of activities performed by the peer group (including the user) in a particular time frame. Botros, column 5, lines 44-61.

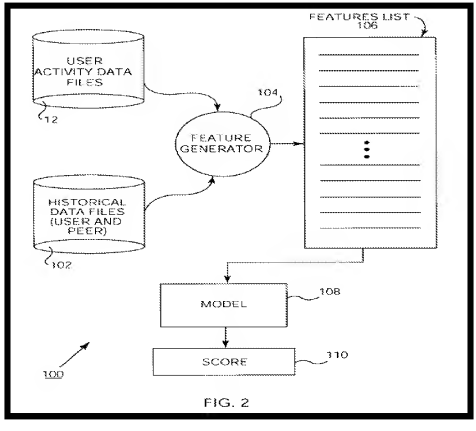


FIG. 2

User activity files 12 and historical data 102 of Botros are used as input to a feature generator or builder 104. The feature generator 104 is implemented involving an equation for

calculating a time-weighted mean. The output from feature generator 104 is a features list 106. The features list 106 contains 47 features which can be classified into several different categories such as violations, user activities, computer and network loads, and so on. Individual features from features list 106 are used as input to a model 108. The model 108 can include processes such as linear regression, Markov models, graphical models, and regression models.

The model 108 of Botros is trained to evaluate features to recognize the possibility of a network intrusion. By training model 108 to process certain types of features, it can recognize potential intrusions. One example of a feature is user login failure, such as the time between login failures for a particular user. Once the model receives all input features, it calculates a score 110. This score is based upon the input features and how the model has been trained. The model 108 is trained using a neural network algorithm. A score 110 can be normalized to a number between 0 and 1000, a high number indicating a stronger possibility of an intrusion. Botros, column 5, line 62 through column 6, line 23.

Botros describes user activity files 12, or the raw user data, which contain raw data of activities performed by users as illustrated in Figure 3 below. User activity files 12 are made up of numerous individual user logs, such as user log 204. The users are on one particular computer system, typically supported by a mainframe computer and operating system. The raw data can also come from several computer systems each supported by different computers. Similarly, score 110 can be derived from data from one or more computer systems and can measure potential intrusions for one or all systems.

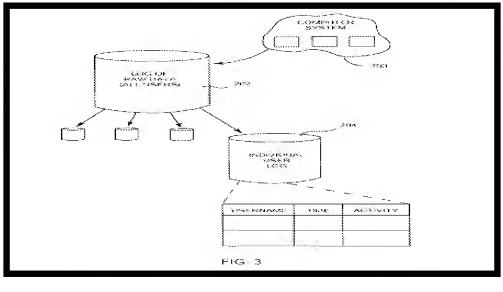


FIG. 3

A computer system 200 of Figure 3 of Botros above contains a number of sources from which raw user activity data is drawn. Examples of these sources or files include operating system files containing executed commands, operations on programs, exceptions, operations on files, and other more data-specific files such as badge-in data. In the described embodiment the sources are maintained by the Multiple Virtual Storage ("MVS") operating system of the IBM Corporation, and used on IBM mainframe computers. These data sources are part of the MVS operating system and are created and maintained as part of the operating system. The process can be used in computer systems using operating systems other than MVS such as a Unix-based operating system. Using the example from above, to determine the time between login failures, the intrusion program checks user activity files 12. Botros, column 6, lines 24-53.

A raw data log 202 contains user activity for all users logged in a particular computer system such as system 200. Computer system 200 parses raw data log 202 according to user and time of activity thereby creating a series of individual user logs, such as user log 204. In the described embodiment, user log 204 is a series of variable length records containing a user name, a timestamp of when the user activity occurred and the name of the specific user activity, as well as other information depending on the user activity or command performed. After data from the system resources is parsed according to user, user activity data is retained or kept in the form of user activity files 12, used as input to feature generator 104. Botros, column 6, lines 53-65. Botros explains that generating user historical data is performed at the end of a user work day for each user logged in and for each computer system in an organization or enterprise. Botros, column 7, lines 1-3.

In view of the passages and Figures 2 and 3 of Botros above, it is clear to one of ordinary skill in the art that Botros is only concerned with historical data and logs of past activity which are analyzed for threats. Botros is opposite to a system which copies packets that are being transmitted in real-time over the computer network and outputting a behavioral rating from respective port modules in real-time. Further, Botros, like Copeland, does not describe or teach processing packets with port modules designed for a single port type and reviewing and comparing information from various parts of each packet, as recited in independent Claim 34.

Summary for Claim 34

Since the cited references in this Office Action fail to teach each and every element claimed in this application, especially those in independent Claim 34, the undersigned representative believes independent Claim 34 and all claims depending therefrom to be allowable over the cited art. Accordingly, the undersigned representative requests consideration and an indication that Claim 34 is allowable over the prior art of record.

Independent Claim 48

It is respectfully submitted that Copeland and Botros, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) a traffic sorter for sorting copied packets based on port type; (2) an activity monitor operatively coupled to the traffic sorter, (3) the activity monitor comprising a plurality of port modules, (4) each port module being designed for processing packets of a single port type and (5) processing packets by reviewing and comparing information from various parts of each packet and (6) determining a presence and absence of port-specific activities based on each packet, (7) each port module outputting a behavioral rating in real-time based, (8) the behavioral rating comprising at least two dimensions of deception and expertise; (9) an inter-port fusion module operatively coupled to the activity monitor for grouping behavioral ratings received from the port modules of the activity monitor; and (10) an outcome director operatively coupled to the inter-port fusion monitor that (11) determines whether to block or track user activities based upon the behavioral ratings received from the inter-port fusion module, as recited in independent Claim 48.

Similar to independent Claim 34, the two references relied on by the Examiner fail to describe or teach an activity monitor comprising a plurality of port modules, each port module being designed for processing packets of a single port type and processing packets by reviewing and comparing information from various parts of each packet.

Since the cited references in this Office Action fail to teach each and every element claimed in this application, especially those in independent Claim 48, the undersigned representative believes independent Claim 48 and all claims depending therefrom to be allowable over the cited art. Accordingly, the undersigned representative requests consideration and an indication that Claim 48 is allowable over the prior art of record.

Independent Claim 51

It is respectfully submitted that Copeland and Botros, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) a computer usable medium having computer readable code embodied therein for preventing unauthorized intrusion into a computer network, the computer program product comprising: (2) computer readable program code configured to cause a computer to copy packets that are being transmitted in real-time over the computer network; (3) computer readable program code configured to cause the computer to sort the copied packets based on port type; (4) computer readable program code configured to cause the computer to process packets of a single port type; (5) computer readable program code configured to cause the computer to process packets by reviewing and comparing information from various parts of each packet; (6) computer readable program code configured to cause the computer to determine a presence and absence of port-specific activities based on the review and comparison of each packet; (7) computer readable program code configured to cause the computer to generate binary vectors representing the presence and absence of port-specific activities based on each packet; (8) computer readable program code configured to cause the computer to assess each binary vector and determine a level of expertise and deception for the port-specific activities represented by the binary vector; and (9) computer readable program code configured to cause the computer to output a behavioral rating from each port module in real-time based on the determining step, (10) the behavioral rating comprising at least two dimensions of deception and expertise, as recited in independent Claim 51.

Similar to independent Claim 34, the two references relied on by the Examiner fail to describe or teach computer readable program code configured to cause a computer to copy packets that are being transmitted in real-time over the computer network; computer readable program code configured to cause the computer to sort the copied packets based on port type; and computer readable program code configured to cause the computer to process packets of a single port type, as recited in independent Claim 51.

Since the cited references in this Office Action fail to teach each and every element claimed in this application, especially those in independent Claim 51, the undersigned representative believes independent Claim 51 and all claims depending therefrom to be allowable over the cited art. Accordingly, the undersigned representative requests consideration and an indication that Claim 51 is allowable over the prior art of record.

Dependent Claims 35-47, 49-50, and 52-53

Since Claims 35-47, 49-50, and 52-53 are dependent on independent Claims 34, 48, and 51 and since these three independent claims are believed to be allowable over the prior art of record, the Applicants believe that these dependent claims are also allowable over the prior art of record. Therefore, the undersigned representative requests consideration and an indication that these dependent claims are allowable over the prior art of record.

CONCLUSION

The undersigned believes that claims in this application are allowable over the cited prior art and respectfully requests a notice of allowance to this effect. Should the Examiner determine that any further action is necessary to place this application into better form, the Examiner is encouraged to telephone the undersigned representative at the number listed below. In addition, if any additional fees are required in connection with the filing of this response, the Commissioner is hereby authorized to charge the same to Deposit Account No. XX-XXXX.

Respectfully submitted,

Date: April 1, 2008

By: */Dawn-Marie Bey - #44,442/*
Dawn-Marie Bey
Registration No. 44,442
(202) 626-8978